



Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

ON THE CLASS NUMBER OF THE FIELD $\Omega(e^{2i\pi/p^n})$ AND THE
SECOND CASE OF FERMAT'S LAST THEOREM

BY H. S. VANDIVER

DEPARTMENT OF MATHEMATICS, CORNELL UNIVERSITY

Communicated by L. E. Dickson, March 31, 1920

In the July 1919 number of the *Bulletin of the American Mathematical Society*, page 458, I gave an expression for the residue of the first factor of the class number of the field defined by $e^{2i\pi/p}$, p being prime, with respect to the modulus p^a , in terms of Bernoulli numbers. In the present paper an analogous expression for the residue of the first factor of the class number of $\Omega(e^{2i\pi/p^n})$ modulo p , will be obtained and the result used to show that certain results due to Bernstein¹ on Fermat's last theorem do not have the generality stated by him. In view of the criticisms on Kummer's 1857 memoir on the last theorem which I have given elsewhere² it is then pointed out that up to the present time no rigorous proof of the theorem for the exponents 59 and 67 has been given.

Westlund³ reduced the first factor of the class number of $\Omega(e^{2i\pi/p^n})$, if $n > 1$, to the form

$$h_1 = k \times \frac{\prod \varphi(\theta^s)}{1/2 p^{n-2}(p-1)^2 \cdot 1/2 n p^{n-2}(p-1)^2 - 1} = k k_1 \quad (1)$$

where k is the first factor of the class number of $\Omega(e^{2i\pi/m^1})$, $\theta = e^{2i\pi/\mu}$, $\mu = \varphi(m) = p^{n-1}(p-1)$, $m = p^n$, $m^1 = p^{n-1}$, r_i is the least positive residue of r^i , modulo p^n , r being a primitive root of p^n . The integer s takes on all odd values $< \mu$ except multiples of p , and the function $\varphi(\theta)$ defined by Westlund may be put in the form

$$\varphi(\theta) = r_0 + r_1\theta + \dots + r_{\mu-1}\theta^{\mu-1}.$$

We shall now reduce k_1 modulo p . To do this a modification of the method used by Kronecker in reducing the first factor of the class number of $\Omega(e^{2i\pi/p})$ will be employed.⁴ We have

$$(r - \theta^{-1})\varphi(\theta) = p^n g(\theta) \quad (2)$$

where

$$g(\theta) = q_0 + q_1\theta + \dots + q_{\mu-1}\theta^{\mu-1}$$

and

$$q_i = \frac{rr_i - r_i + 1}{p^n}.$$

From an argument used by Westlund we also have

$$\prod_s (r - \theta^{-s}) = \frac{r^{\frac{\mu}{2}} + 1}{r^{\frac{\mu^1}{2}} + 1},$$

where $\mu^1 = \varphi(m^1)$. Since r is a primitive root of p^n , then $r^{\frac{\mu^1}{2}} = -1 +$

$p^{n-1}a$, where a is prime to p . Hence $r^{\frac{\mu}{2}} = (-1 + p^{n-1}a)^p = -1 + p^n a + p^{2n-1}a_1$, where a_1 is a multiple $a_2 a$ of a . Thus

$$\Pi_s(r - \theta^{-s}) = \frac{p^n a + p^{2n-1} a_1}{p^{n-1} a} = p + p^n a_2,$$

whence

$$(1 + a_2 p^{n-1}) \frac{\Pi_s \varphi(\theta^s)}{1/2 n p^{n-2} (p-1)^2 - 1} \equiv \Pi_s g(\theta^s)$$

and since

$$2^{1/2} p^{n-2} (p-1)^2 \equiv 1 \pmod{p},$$

we have

$$k_1 \equiv \Pi_s g(\theta^s) \pmod{p}. \quad (3)$$

Now $\Pi_s g(\theta^s) = a$, where a is a rational integer. Consider the expression $\Pi_s g(x^s) - a$, where x is an indeterminate. This is a polynomial in x which vanishes for $x = \theta$, and hence is divisible by $V(x) = \prod_i (x - \theta^i)$, i ranging over the $\varphi(\mu)$ integers less than and prime to μ , since $V(x)$ is irreducible in the domain of rational integers. We write then

$$\Pi_s g(x^s) = a + V(x)W(x), \quad (4)$$

where $W(x)$ is a rational integral function of x . Let

$$V_s = V_s(x) = \prod_i (x - \omega^i)$$

where i ranges over all the integers less than s and prime to it, and ω is a primitive s^{th} root of unity. Then

$$\frac{x^\mu - 1}{x^{\mu'} - 1} = V_\mu V_{c_1} V_{c_2} \dots, \quad (5)$$

where $c_1, c_2, \dots$ are all the numbers of the form $p^{n-1}k$, where k is a divisor of $p-1$ which is $< p-1$. Since r is a primitive root of p^n it is also a primitive root of p . Also, (5) gives

$$\frac{r^\mu - 1}{r^{\mu'} - 1} = V_\mu(r) V_{c_1}(r) V_{c_2}(r) \dots \quad (6)$$

Now no V_c can be divisible by p since it would then follow that

$$r^c \equiv 1 \pmod{p}$$

which is impossible since c is not a multiple of $p-1$. Since the left-hand member of (6) is divisible by p , we, therefore, conclude that $V_\mu(r) \equiv 0 \pmod{p}$. Substituting $x = r$ in (4) and using (3), we have

$$k_1 \equiv \Pi_s g(r^s) \pmod{p}. \quad (7)$$

By Fermat's theorem we have

$$\prod_s g(r^s) \equiv \prod_t (g(r^{2t-1}))^{p^n - 2(p-1)} \pmod{p}, \quad (7a)$$

where $t = 1, 2, \dots, \frac{p-1}{2}$. To reduce $g(r^{2t-1})$ modulo p , we have

$$rr_i = r_{i+1} + rr_i - r_{i+1}$$

Raising to the power $2t$, and noting that $rr_i - r_{i+1} \equiv 0 \pmod{p^n}$, we get

$$r^{2t} r_i^{2t} \equiv r_{i+1}^{2t} + 2t(rr_i - r_{i+1})r_{i+1}^{2t-1} \pmod{p^{2n}}.$$

Transposing, we have

$$2tr_{i+1}^{2t-1}(rr_i - r_{i+1}) \equiv r^{2t} r_i^{2t} - r_{i+1}^{2t} \pmod{p^{2n}}.$$

But, by definition,

$$r_{i+1} \equiv r^{i+1} \pmod{p^n}$$

and therefore

$$(rr_i - r_{i+1})r_{i+1}^{2t-1} \equiv (rr_i - r_{i+1})r^{(i+1)(2t-1)} \pmod{p^{2n}},$$

whence, if $i = 0, 1, \dots, \mu-1$,

$$2tp_n r^{2t-1} \sum_i q_i r^{i(2t-1)} \equiv r^{2t} \sum_i r_i^{2t} - \sum_i r_{i+1}^{2t} \pmod{p^{2n}}.$$

Now

$$\sum r_i^{2t} = \sum r_{i+1}^{2t} = a_1^{2t} + a_2^{2t} + \dots + a_\mu^{2t} = S_{2t},$$

where the a 's are the integers less than p^n and prime to it. Hence

$$\prod_t (r^{2t-1}) \equiv \prod_t \frac{(r^{2t}-1)S_{2t}}{2tp_n r^{2t-1}} \pmod{p}. \quad (8)$$

To reduce the expression on the right-hand side we shall first consider the quantity S_{2t} . It will be shown that

$$S_{2t} \equiv R_{2t} \pmod{p^{n+1}} \quad (9)$$

for $t < (p-1)/2$ and

$$S_{2t} \equiv R_{2t} \pmod{p^n} \quad (9a)$$

for $t = (p-1)/2$, where

$$R_{2t} = 1^{2t} + 2^{2t} + \dots + (p^n - 1)^{2t}.$$

We have

$$\begin{aligned} S_{2t} &= R_{2t} - (p^{2t} + (2p)^{2t} + (3p)^{2t} + \dots + (p^n - p)^{2t}) \\ &= R_{2t} - p^{2t}(1^{2t} + 2^{2t} + \dots + (p^{n-1} - 1)^{2t}). \end{aligned} \quad (9b)$$

Now

$$T_{2t} = 1^{2t} + 2^{2t} + \dots + (p^{n-1} - 1)^{2t} \equiv 0 \pmod{p^{n-1}}$$

for $t < (p-1)/2$ and

$$T_{p-1} \equiv 0 \pmod{p^{n-2}}.$$

To show this let k be a primitive root of p^{n-1} , then $k^{2t}T_{2t} \equiv T_{2t} \pmod{p^{n-1}}$ and

$$(k^{2t} - 1)T_{2t} \equiv 0 \pmod{p^{n-1}}.$$

In this relation $k^{2t} - 1$ is prime to p for $t < (p-1)/2$ and for $2t = p-1$, $k^{2t} - 1$ is divisible by p but not by p^2 . Hence

$$T_{2t} \equiv 0 \pmod{p^{n-1}}$$

for $2t < p - 1$ and

$$T_{p-1} \equiv 0 \pmod{p^{n-2}}. \quad (9c)$$

Applying these to (9b), the relations (9) and (9a) follow. We also have by the Bernoulli summation formula

$$R_{2t} = \frac{p^{n(2t+1)}}{2t+1} + \frac{p^{2tn}}{2} + \binom{2t}{1} \frac{B_1}{2} p^{n(2t-1)} \\ - \binom{2t}{3} \frac{B_2}{4} p^{n(2t-3)} + \dots + (-1)^{t+1} B_t p^n.$$

where $B_1 = 1/6$, $B_2 = 1/30$, etc.

By the von Staudt-Clausen theorem, the Bernoulli numbers $B_1, B_2, \dots, B_{(p-3)/2}$ all have denominators prime to p . Hence if $2t < p - 1$ every term in the above expansion is an integer, or else a fraction whose denominator is prime to p . Also the numerators except in the last term, are divisible by p^{2n} . If $2t = p - 1$, then the denominator of B_{p-1} is divisible by p but not by p^2 and, therefore, we may write

$$R_{p-1} \equiv p^{n-1} a \pmod{p^{2n}} \quad (a \text{ an integer prime to } p). \quad (10)$$

Hence we may write

$$R_{2t} \equiv (-1)^{t+1} B_t p^n \pmod{p^{n+1}}$$

and, therefore, for any $t < (p-1)/2$ we have

$$\frac{(r^{2t}-1)S_{2t}}{2tp^n r^{2t}-1} \equiv \frac{(r^{2t}-1)R_{2t}}{2tp^n r^{2t}-1} \equiv \frac{(-1)^{t+1} B_t (r^{2t}-1)}{2tr^{2t}-1} \pmod{p} \quad (11)$$

For $t = (p-1)/2$, the corresponding factor in the right-hand member of (8) takes the form

$$\frac{(r^{p-1}-1)S_{p-1}}{(p-1)p^n r^{p-2}}. \quad (11a)$$

We have from (9a)

$$S_{p-1} \equiv R_{p-1} \pmod{p^n}$$

and, therefore, the relation (10) shows that $(r^{p-1}-1)S_{p-1}$ is divisible by p^n but not by p^{n+1} since $r^{p-1}-1$ is divisible by p but not by p^2 . Then modulo p , the expression (11a) may be reduced to an integer prime to p . Using this in connection with (11), (7a) and (8), we obtain

$$\prod_s g(r^s) \equiv \left(\prod_{t=1}^{(p-3)/2} B_t \right)^{p^n - 2(p-1)} \pmod{p}. \quad (12)$$

Hence, $\prod_s g(r^s)$ and, therefore, k , is divisible by p if and only if at least one of the numbers B_t ($t = 1, 2, \dots, (p-3)/2$) is divisible by p . (A Bernoulli number is said to be divisible by an integer i when its denominator is prime to i and its numerator is divisible by i .) Now Bernstein in his article cited above gives the result:

Under the assumption that the class number of $\Omega(e^{2i\pi/p^2})$ is divisible by p but not by p^2 , the relation

$$x^p + y^p + z^p = 0 \quad (13)$$

is impossible in integers prime to each other if $xyz \equiv 0 \pmod{p}$.

I shall now show that this criterion constitutes no extension over the one given by Kummer to the effect that (13) is impossible in integers if p is a regular prime. For if the former applies to other than regular primes as exponents, then p must be a prime such that

$$\prod_{i=1}^{(p-3)/2} B_i \equiv 0 \pmod{p}.$$

This being the case, it follows from (12) that $k_1 \equiv 0 \pmod{p}$, and by Kummer's theorem,⁵ k is also divisible by p . Hence $h_1 \equiv 0 \pmod{p^2}$ contrary to Bernstein's assumption that the class number of $\Omega(e^{2i\pi/p^2})$ is not divisible by p^2 .

In a paper cited above the writer pointed out errors in Kummer's memoir of 1857 on the relation (13). Considering this in connection with the failure of Bernstein's criterion it follows that Fermat's last theorem has not been rigorously proved for all non-regular primes less than 100. These non-regular primes are 37, 59 and 67. Mirimanoff⁶ gave an adequate proof for the case $p = 37$, which leaves the cases $p = 59$ and 67 still to be disposed of.

In connection with the cyclotomic class number it may be noted that Furtwängler⁷ proved that the class number of $\Omega(e^{2i\pi/p^n})$ is divisible by the prime p if, and only if, the first factor of the class number of the field $\Omega(e^{2i\pi/p})$ is divisible by p .

2. Bernstein⁸ also gave a criterion in connection with (13) for the case where x , y and z are prime to p . He makes two assumptions the first being to the effect that the *second* factor of the class number of $\Omega(e^{2i\pi/p})$ is divisible by p , and states *l. c.*, p. 507, that his criterion includes that of Kummer's 1857 memoir as a special case. This is not correct, however, as there are no primes, p less than 100 such that the 2nd factor of the class number is divisible by p . (This follows from some computations by Kummer⁹ in connection with certain investigations regarding the last theorem.) This being the case, Bernstein's criterion can at most supplement Kummer's which latter criterion stated that if (13) is satisfied in integers such that xyz is prime to p then $B_{(p-3)/3}$ and $B_{(p-5)/2}$ are divisible¹⁰ by p .

This criterion would eliminate, for example, all p 's less than 100, which Bernstein's condition does not do.

3. Kummer¹¹ rigorously established the theorem that (13) cannot be satisfied in integers prime to each other if p is a regular prime, and noted that all primes < 100 were regular except 37, 59 and 67. But Kummer¹² also showed that the first factor of the class numbers of $\Omega(e^{2i\pi/p})$ for all primes p , where $100 < p < 167$, excepting $p = 101, 103, 131, 149$ and 157, was in each case prime to p .¹³ It follows that the primes p which are

> 100 and < 167 with the exceptions noted above are all regular and the last theorem is proved for these exponents p .

¹ *Göttingen Nachrichten*, 1910 (507-16).

² These PROCEEDINGS, 6, 1920 (266).

³ *Trans. Amer. Math. Soc.*, 4, 1903 (201-12).

⁴ Hilbert, *Die Theorie der Algebraischen Zahlkörpers*, p. 430.

⁵ Hilbert, *l. c.*, p. 429.

⁶ *Crelle*, 111, 1893 (26-30).

⁷ *Ibid.*, 140, 1911 (29).

⁸ *L. c.*, pp. 482-88.

⁹ *Abhandlungen Berlin Academy*, 1857, p. 73, verification of 2nd assumption.

¹⁰ Kummer, *l. c.*, pp. 63-5.

¹¹ *Crelle*, 40 (93-139).

¹² *Berlin Monatsberichte*, 1874.

¹³ Hilbert, *l. c.*, pp. 429, 435.

OBSERVATIONS ON THE STERILITY OF MUTANT HYBRIDS IN *DROSOPHILA VIRILIS*

By C. W. METZ

STATION FOR EXPERIMENTAL EVOLUTION, CARNEGIE INSTITUTION OF WASHINGTON

Communicated by C. B. Davenport, May 28, 1920

In an earlier paper¹ by Metz and Bridges, attention was called to two cases of apparent incompatibility between mutant races in *Drosophila*. One of these cases involved my data on the sex linked characters rugose and glazed in *Drosophila virilis*. Subsequent to the publication of this paper another character appeared in *D. virilis* that shows the same relations to rugose and glazed that they do to one another.² A study of these three characters has brought out some interesting relationships and has apparently revealed an error in the previous publication that should be corrected.

It may be recalled that hybrids between rugose and glazed were invariably sterile, while supposedly pure stock of each mutant was fertile and hybrids of either with other mutant stocks were fertile; hence it was concluded that rugose and glazed were incompatible. It appears now that a mistake was probably made in the statement that pure stocks of both rugose and glazed have normal fertility. Apparently this should have applied only to rugose, for later work has shown that females homozygous for glazed are usually sterile and that pure cultures cannot be maintained—at least without great difficulty. Possibly this condition has arisen by the secondary appearance of sterility factors in the stock since the previous paper was written, but more probably the earlier stock was impure, at least part of the time—the impurity having been overlooked through confusion with rugose in which the homozygous females are somatically normal. Unfortunately no accurate records of stock